



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/063,891	05/22/2002	Kun-Huei Chen	IACP0004USA	2371

27765 7590 05/24/2006

NORTH AMERICA INTELLECTUAL PROPERTY CORPORATION
P.O. BOX 506
MERRIFIELD, VA 22116

EXAMINER

DAVIS, ZACHARY A

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 05/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/063,891	Applicant(s) CHEN ET AL.	
	Examiner Zachary A. Davis	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 March 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-9 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-9 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 22 May 2002 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. An amendment was received on 13 March 2006. By this amendment, Claims 1 and 6 have been amended. No claims have been added or canceled. Claims 1-9 are currently pending in the present application.

Specification

2. The Examiner thanks Applicant for the changes in replacing the term "detonate" throughout the specification. However, the Examiner notes that the amendments have introduced at least one new error as noted below. Further, as noted in the following section, the drawings also include the term "detonate" and should also be corrected.

3. The disclosure is objected to because of the following informalities:

The specification appears to contain minor errors. Specifically, in paragraph 0054, as amended by the present response, it appears that in the phrase "random-code generation program 38 is activates", "activates" is intended to read "activated".

Appropriate correction is required. Applicant's cooperation is again requested in correcting any other errors of which Applicant may become aware in the specification.

Drawings

4. The drawings are objected to because they include the term “detonate” (see Figure 3, step 100). It appears that this should be corrected, as has been done elsewhere in the disclosure, to read “activate”. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet” pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

5. The rejection of Claims 1-9 under 35 U.S.C. 112, second paragraph, as indefinite is withdrawn in light of the amendments to the claims.

Response to Arguments

6. Applicant's arguments filed 13 March 2006 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 1-9 under 35 U.S.C. 103(a) as unpatentable over Duda, US Patent 5708710 in view of Kung et al, US Patent 6889321, Applicant argues that neither Duda nor Kung teaches encrypting the second ciphering key with the first cipher key before transmitting the second ciphering key. However, the Examiner respectfully disagrees, noting that Kung discloses that a second key is distributed encrypted by a first key (see Figure 10; see also column 35, line 61-column 36, line 20) and that Kung further discloses that updates of the encryption key can occur when the secure feature is active (and therefore new keys which are distributed are implicitly encrypted by the old key; see column 34, lines 44-47; see also column 33, lines 14-17, where *all* communication is encrypted using a key). The Examiner further notes that Duda generally discloses that specific details of techniques for updating encryption keys are known in the art (see column 5, lines 39-43).

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 1-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Duda, US Patent 5708710 in view of Kung et al, US Patent 6889321.

In reference to Claim 1, Duda discloses a method for updating a ciphering key used in a wireless network system (see, for example, column 3, lines 31-38) where the method includes starting a counter (column 4, lines 43-48), randomly generating a second key (see column 4, lines 10-12) if the counter conforms to a predetermined threshold (column 4, lines 53-55), a wireless access point transmitting the second key to a wireless station to update a first key stored in the station, and using the updated key to encrypt data between the access point and the station (column 5, lines 34-39). However, although Duda discloses a counter and a counter threshold as described above, Duda does not explicitly disclose that the counter counts a time and that the key is updated at a predetermined time.

Kung discloses a system in which a randomly generated encryption key (column 33, lines 8-11) in a wireless system (see, for example, column 5, lines 14-19) is updated at predetermined time intervals, either a set interval or random sized intervals (column 34, lines 25-43). Kung further discloses that the second key is encrypted by the first key when updating (Figure 10; column 35, line 61-column 36, line 20; column 34, lines 44-47). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Duda to include a clock counting a specific time as the counter, in order to prevent a compromised key from causing excessive damage by limiting the length of time an exposed key would remain active (see Kung, column 34, lines 43-46, where a hacker with access to a broken key is prevented from having continuous access to the system).

In reference to Claims 2 and 3, Duda and Kung further disclose transmitting a challenge text from the access point to the station; the station encrypting the challenge text into the response text which is transmitted to the access point; the access point comparing the response text to a standard text, which is also the encrypted challenge text (see Duda, column 2, lines 22-32, where a well-known challenge response method is used); the station transmitting identification data to the access point and thereby to a server; and the access point updating the key if the identification data matches data stored in the server (see Duda, column 1, lines 39-50; column 3, lines 45-52; column 4, lines 18-27).

In reference to Claim 4, Duda and Kung further disclose requesting a response from a user before updating the key (see Duda, column 2, lines 22-32).

In reference to Claim 5, Duda and Kung further disclose decrypting data using the second key once the key is updated (Duda, column 5, lines 34-39, where the key is updated).

In reference to Claim 6, Duda and Kung further disclose a plurality of stations, each storing a key and a unique identification data (for example, Duda, column 1, lines 39-48; column 3, lines 45-67).

In reference to Claim 7, Duda and Kung further disclose generating the key randomly (Duda, column 4, lines 10-12; Kung, column 33, lines 8-11).

In reference to Claim 8, Duda and Kung further disclose the access point transmitting a challenge text to the station after the key is updated, and performing a well-known challenge response protocol to verify the second key has been properly received and updated (see Duda, column 2, lines 22-32).

In reference to Claim 9, Duda and Kung further disclose a real time clock (Kung, column 9, lines 55-62).

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not

Art Unit: 2137

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER